European Commission

Questions and answers | 10 July 2023 | Brussels

Questions & Answers: EU-US Data Privacy Framework

On 10 July, the European Commission adopted its adequacy decision for the EU-U.S. Data Privacy Framework. The adequacy decision concludes that the United States ensures an adequate level of protection – compared to that of the EU - for personal data transferred from the EU to US companies participating in the EU-U.S. Data Privacy Framework.

The adequacy decision follows the US' signature of an Executive Order on 'Enhancing Safeguards for United States Signals Intelligence Activities', which introduced new binding safeguards to address the points raised by Court of Justice of the European Union in its Schrems II decision of July 2020. Notably, the new obligations were geared to ensure that data can be accessed by US intelligence agencies only to the extent of what is necessary and proportionate, and to establish an independent and impartial redress mechanism to handle and resolve complaints from Europeans concerning the collection of their data for national security purposes.

1. What is an adequacy decision?

An adequacy decision is one of the tools provided under the General Data Protection Regulation (GDPR) to transfer personal data from the EU to third countries which, in the assessment of the Commission, offer a comparable level of protection of personal data to that of the European Union.

As a result of adequacy decisions, personal data can flow freely and safely from the European Economic Area (EEA), which includes the 27 EU Member States as well as Norway, Iceland and Liechtenstein, to a third country, without being subject to any further conditions or authorisations. In other words, transfers to the third country can be handled in the same way as intra-EU transmissions of data.

The adequacy decision on the EU-U.S. Data Privacy Framework covers data transfers from any public or private entity in the EEA to US companies participating in the EU-U.S. Data Privacy Framework.

2. What are the criteria to assess adequacy?

Adequacy does not require the third country's data protection system to be identical to the one of the EU, but is based on the standard of ‘essential equivalence'. It involves a comprehensive assessment of a country's data protection framework, both of the protection applicable to personal data and of the available oversight and redress mechanisms.

The European data protection authorities have developed a list of elements that must be taken into account for this assessment, such as the existence of core data protection principles, individual rights, independent supervision and effective remedies.

3. What is the EU-U.S. Data Privacy Framework?

In its adequacy decision, the Commission has carefully assessed the requirements that follow from the EU-U.S. Data Privacy Framework, as well as the limitations and safeguards that apply when personal data transferred to the US would be accessed by US public authorities, in particular for criminal law enforcement and national security purposes.

On that basis, the adequacy decision concludes that the United States ensures an adequate level of protection for personal data transferred from the EU to companies participating in the EU-U.S. Data Privacy Framework. With the adoption of the adequacy decision, European entities are able to transfer personal data to participating companies in

the United States, without having to put in place additional data protection safeguards.

The Framework provides EU individuals whose data would be transferred to participating companies in the US with several new rights (e.g. to obtain access to their data, or obtain correction or deletion of incorrect or unlawfully handled data). In addition, it offers different redress avenues in case their data is wrongly handled, including before free of charge independent dispute resolution mechanisms and an arbitration panel.

US companies can certify their participation in the EU-U.S. Data Privacy Framework by committing to comply with a detailed set of privacy obligations. This could include, for example, privacy principles such as purpose limitation, data minimisation and data retention, as well as specific obligations concerning data security and the sharing of data with third parties.

The Framework will be administered by the US Department of Commerce, which will process applications for certification and monitor whether participating companies continue to meet the certification requirements. Compliance by US companies with their obligations under the EU-U.S. Data Privacy Framework will be enforced by the US Federal Trade Commission.

4. What are the limitations and safeguards regarding access to data by United States intelligence agencies?

An essential element of the US legal framework on which the adequacy decision is based concerns Executive Order on ‘Enhancing Safeguards for United States Signals Intelligence Activities', which was signed by President Biden on 7 October and is accompanied by regulations adopted by the Attorney General. These instruments were adopted to address the issues raised by the Court of Justice in its Schrems II judgment.

For Europeans whose personal data is transferred to the US, the Executive Order provides for:

- Binding safeguards that limit access to data by US intelligence authorities to what is necessary and proportionate to protect national security;
- Enhanced oversight of activities by US intelligence services to ensure compliance with limitations on surveillance activities; and
- The establishment of an independent and impartial redress mechanism, which includes a new Data Protection Review Court to investigate and resolve complaints regarding access to their data by US national security authorities.

5. What is the new redress mechanism in the area of national security and how can individuals make use of it?

The US Government has established a new two-layer redress mechanism, with independent and binding authority, to handle and resolve complaints from any individual whose data has been transferred from the EEA to companies in the US about the collection and use of their data by US intelligence agencies.

For a complaint to be admissible, individuals do not need to demonstrate that their data was in fact collected by US intelligence agencies. Individuals can submit a complaint to their national data protection authority, which will ensure that the complaint will be properly transmitted and that any further information relating to the procedure —including on the outcome—is provided to the individual. This ensures that individuals can turn to an authority close to home, in their own language. Complaints will be transmitted to the United States by the European Data Protection Board.

First, complaints will be investigated by the so-called ‘Civil Liberties Protection Officer' of the US intelligence community. This person is responsible for ensuring compliance by US intelligence agencies with privacy and fundamental rights.

Second, individuals have the possibility to appeal the decision of the Civil Liberties Protection Officer before the newly created Data Protection Review Court (DPRC). The Court is composed of members from outside the US Government, who are appointed on the basis of specific

qualifications, can only be dismissed for cause (such as a criminal conviction, or being deemed mentally or physically unfit to perform their tasks) and cannot receive instructions from the government. The DPRC has powers to investigate complaints from EU individuals, including to obtain relevant information from intelligence agencies, and can take binding remedial decisions. For example, if the DPRC would find that data was collected in violation of the safeguards provided in the Executive Order, it can order the deletion of the data.

In each case, the Court will select a special advocate with relevant experience to support the Court, who will ensure that the complainant's interests are represented and that the Court is well informed of the factual and legal aspects of the case. This will ensure that both sides are represented, and introduce important guarantees in terms of fair trial and due process.

Once the the Civil Liberties Protection Officer or the DPRC completes the investigation, the the complainant will be informed that either no violation of US law was identified, or that a violation was found and remedied. At a later stage, the complainant will also be informed when any information about the procedure before the DPRC—such as the reasoned decision of the Court— is no longer subject to confidentiality requirements and can be obtained.

6. When will the decision apply?

The adequacy decision entered into force with its adoption on 10 July.

There is no time limitation, but the Commission will continuously monitor relevant developments in the United States and regularly review the adequacy decision.

The first review will take place within one year after the entry into force of the adequacy decision, to verify whether all relevant elements of the US legal framework are functioning effectively in practice. Subsequently, and depending on the outcome of that first review, the Commission will decide, in consultation with the EU Member States and data protection authorities, on the periodicity of future reviews, which will take place at least every four years.

Adequacy decisions can be adapted or even withdrawn in case of developments affecting the level of protection in the third country.

7. What is the impact of the decision on the possibility to use other tools for data transfers to the United States?

All the safeguards that have been put in place by the US Government in the area of national security (including the redress mechanism) apply to all data transfers under the GDPR to companies in the US, regardless of the transfer mechanims used. These safeguards therefore also faciliate the use of other tools, such as standard contractual clauses and binding corporate rules.

For more information

Adequacy decision on the EU-US Data Privacy Framework

Press release

Factsheet – Transatlantic Data Privacy Framework

EU-US data transfers (europa.eu)

International dimension of data protection (europa.eu)

Adequacy decisions (europa.eu)

Joint Statement on Trans-Atlantic Data Privacy Framework (europa.eu)

Contacts for media

Christian WIGAND

Phone

+32 2 296 22 53

Mail

christian.wigand@ec.europa.eu

Cristina TORRES CASTILLO

Phone

+32 2 29 90679

Mail

Cristina.TORRES-CASTILLO@ec.europa.eu

If you do not work for a media organisation, you are welcome to contact the EU through Europe Direct in writing or by calling 00 800 6 7 8 9 10 11.

QANDA/23/3752